Notice of Allowability	Application No.	Applicant(s)	
	09/654,638	TAKAGI ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed 11/09/2004 and examiner's amendment on 523/2005*.

2. ☒ The allowed claim(s) is/are *1-5,8,9,13,17 and 21*.

3. ☒ The drawings filed on *05 September 2000* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

S.O.O.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brenda Holmes on 5/23/2005.

The application has been amended as follows:

2. (Currently Amended) A signer device for processing an undeniable digital signature, the signer device implemented using a computer, comprising:

a key generation unit for generating public keys (D, P, k, t) and secret keys (D1, q), by generating two primes p, q ($p, q > 4$, $p = 3 \bmod 4$, $\sqrt{\frac{p}{3}} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\frac{\sqrt{|D1|}}{4}$ and a bit length t of q-(D1/q) where (D1/q) denotes Kronecker symbol, and generating a kernel element P of a map from a class group Cl(D) to a class group Cl(D1);

a signature generation unit for generating a signature S for a message m, by embedding the message m into a message ideal M in the class group Cl(D) where a norm of the message ideal M is larger than k+1 bits, and mapping the message ideal M to the class group Cl(D1) and pulling the mapped message ideal M back to the class group Cl(D); and

a response generation unit for receiving a challenge C = BH from a verifier side, where B is a random ideal whose norm is smaller than k-1 bits, $H = (M/S)^r$, and r is a random integer smaller than t bits, computing a response W by mapping the challenge C to the class group Cl(D1) and pulling the mapped challenge C back to the class group Cl(D) and squaring a result of mapping and pulling back, using the secret keys (D1, q), and sending the response W to the verifier side, in a process for verifying the signature S.

3. (Currently Amended) A verifier device for processing an undeniable digital signature, using a message m and a signature S for the message m received from a signer side, the verifier device implemented using a computer, where public keys (D, P, k, t) and secret keys (D1, q) are defined by generating two primes p, q (p, $q > 4$, $p = 3 \bmod 4$, $\sqrt{\frac{p}{3}} < q$), computing $D1 = -p$ and $D = D1q^2$, obtaining a bit length k of $\frac{\sqrt{|D1|}}{4}$ and a bit length t of q-(D1/q) where (D1/q) denotes Kronecker symbol, and generating a kernel element P of a map from a class group Cl(D) to a class group Cl(D1), and the signature S is generated by embedding the message m into a message ideal M in the class group Cl(D) where a norm of the message ideal M is larger than k+1 bits, and mapping the message ideal M to the class group Cl(D1) and pulling the mapped message ideal M back to the class group Cl(D), the verifier device comprising:

a norm checking unit for checking whether a norm N(S) of the signature S is smaller than k bits or not, and judging that the signature S is illegal when the norm N(S) is larger than k bits;

a challenge generation unit for generating a challenge C when the norm N(S) is not larger than k bits, by computing the message ideal M of the message m, generating a random integer r smaller than t bits, computing $H = (M/S)^r$, generating a random ideal B whose norm is smaller than k-1 bits, and computing a challenge $C = BH$, and for sending the challenge C to the signer side; and

a response checking unit for receiving a response W from the signer side, checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, where the response W being obtained by mapping the challenge C to the class group Cl(D1) and pulling the mapped challenge C back to the class group Cl(D) and squaring a result of mapping and pulling back, using the secret keys (D1, q).

2. The following is an examiner's statement of reasons for allowance. The present invention is directed to a method for generating and verifying an undeniable signature based on a quadratic field. More specifically, independent claims 1-5, 8, 13, 17 and 21 identify the uniquely distinct steps in the signature verification process: (c2) computing a response W by mapping the challenge C to the class group Cl(D1) and pulling the mapped challenge C back to the class group Cl(D) and squaring a result of mapping and pulling back, using the secret keys (D1, q), at the signer side; and (c3) checking whether $W = B^2$ holds or not, and judging that the signature S is legal when $W = B^2$ holds or that the signature S is illegal otherwise, at the verifier side. The closest prior art, Biehl et al ("Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders"), discloses a method for generating an undeniable signature based on a quadratic field. However, the Biehl reference uses a different protocol for the signature verification process, which does not employ the specific steps mentioned above. The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
5/24/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100